



Secure Wireless Management

PRESS RELEASE

Contact:

Drew Tick
Code Red Systems
Tel: +972-2-642-3401, ext. 100
Cell: +972-54-453-3798
Fax: +972-2-678-3403
Email: drew.tick@code-red.biz

FOR IMMEDIATE RELEASE

October 16, 2007

CODE RED INTRODUCES “STICKY WIRELESS”™ SOFTWARE

Security application ensures that corporate users connect only to authorized secure WiFi networks

Jerusalem, Israel (October 16th, 2007) – Code Red Systems, a leading developer of command and control software for wireless networks, unveiled the latest version of their AirStop Endpoint Security software including some significant enhancements. Among the new features is their “Sticky Wireless” technology which forces users to “stick” to a particular wireless network and prevents connection to unauthorized wireless networks. The software is used to enforce corporate wireless security policy by enabling system administrators to define one or more authorized secure networks. Mobile users are then forced to connect to the authorized networks and will be disconnected if an attempt is made to connect to an unauthorized network.

The market need for Sticky Wireless was first brought Code Red’s attention by PCS Security, a well known provider of data security solutions for the Government of Singapore. It seems that on the island of Singapore there is a municipal WiFi network with extensive coverage. The problem started when corporate users attempted to connect to their secure corporate networks and instead were connecting automatically to the insecure public network. The solution called for a way to make sure that users connected only to the secure corporate wireless network and prevented connection to other networks.

Code Red’s engineers felt the best way to provide this solution was by integrating their AirBlock® technology with their existing AirStop® product. The AirStop software already provides a mechanism for controlling communications adapters and storage devices on laptop computers, so it



Secure Wireless Management

seemed natural to add “Sticky Wireless” functionality which would result in a more robust and comprehensive endpoint security solution.

“We were already familiar with Code Red’s anti-bridging technology.” said Hoo Ming, Managing Directory of PCS Security “and figured that they would be best equipped to provide a solution according to the stringent specifications of the Singaporean Government.”

Through their mutual connection with Ramot Consulting, a firm specializing in bringing Israeli technology to Asian markets, PCS was connected to Code Red’s Jerusalem office and were pleased by the company’s ability to provide the required feature in a minimal time frame. The product was introduced at the recent government data security conference in Singapore and now being considered by a number of agencies.

“We were aware of the problem and already know how to implement the “Sticky Wireless” solution based on a combination of our existing technologies”, said Drew Tick the CEO of Code Red Systems, “Once we saw interest from a respected player in the Asian data security market such as PCS, we felt the time was right to implement this important feature.”

The standard AirStop software, including the anti-bridging technology, is currently available on a 30-day trial basis from most major software download sites. A trial of the enhanced version including the “Sticky Wireless” functionality is available directly from Code Red and its authorized distributors.

About Code Red Systems:

Code Red is a software developer specializing in management and security solutions for wireless networks. The company is headquartered in Jerusalem, Israel, and has a staff of software engineers with hands-on military and civilian data management and security experience. For more information please visit the company web site at: <http://www.code-red.biz>